STATEWIDE INFORMATION TECHNOLOGY ARCHITECTURE PAPER

Architecture Paper: Montana Enterprise Information Technology Security Architecture

Effective Date: January 1, 2008

Approved: Richard B. Clark

Replaces & Supercedes: None

I. Purpose

The purpose of the *Montana Enterprise Information Technology Security Architecture* (hereafter known as the Montana Security Architecture) is to define the basis of the Department of Administration, Information Technology Services Division's (ITSD) security architecture.

ITSD has adopted this architecture as the model and framework of information technology security best practices to implement the security responsibilities of the Department of Administration as required by the Montana Information Technology Act.

Because this architecture was derived from national and industry architectural standards of best practice, implementing the architecture best positions the department to align with current, emerging and anticipated Federal requirements for information technology.

II. Definition(s)

Refer to the Statewide Information Technology Policies and Standards Glossary for a complete list of definitions.

III. Closing

For questions or change requests on this architecture paper, please e-mail ITpolicy@mt.gov.

Or, you may contact the Information Technology Services Division at:

PO Box 200113
Helena, MT 59620-0113
(406) 444-2700

IV. Cross-Reference Guide

A. Architecture Documents

- Montana Information Technology Act 2-17-534. http://data.opi.mt.gov/bills/mca/2/17/2-17-534.htm
- Security responsibilities of departments for data MCA 2-15-114 http://data.opi.mt.gov/bills/mca/2/15/2-15-114.htm
- US FEAF http://www.whitehouse.gov/omb/egov/a-1-fea.html
- FISMA http://csrc.nist.gov/sec-cert/index.html
- FIPS 199 http://csrc.nist.gov/publications/fips/#fips199
- FIPS 200 http://csrc.nist.gov/publications/fips/#fips200
- NIST Special Publication 800-37
- NIST Special Publication 800-53 Revision 1
- NIST Special Publication 800-53A
- NIST Special Publication 800-60

V. Administrative Use

History Log	
Document ID:	ARCH-20070612a
Version:	1.0
Approved Date:	
Effective Date:	January 1, 2008
Change & Review Contact:	ITpolicy@mt.gov
Review:	Event Review: Any event affecting this architecture paper may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	Five years from Effective Date
Last Review/Revision:	
Changes:	

Draft – #4 - 6/27/2007

State of Montana

Montana Enterprise Information Technology Security Architecture

June 2007

Office of the Chief Information Officer
Department of Administration
Information Technology Services Division

TABLE OF CONTENTS

I. Executive Summary

The Montana Security Architecture is an integral and critical domain designed specifically to:

- enable secure communications and the appropriate protection of information resources within the State;
- support the legal information security requirements established by existing Federal and State statutes pertaining to information confidentiality, integrity, availability, and privacy;
- support secure, efficient transaction of business and delivery of services;
- leverage opportunities to obtain IT security synergies and economies of scale.

Accordingly, the Montana Security Architecture supports the overarching goal of an enterprise architecture to enable and accelerate the development of the framework that aligns information technology resources with business strategies, and fosters effective and timely technical decision-making.

The relative significance of the Montana Security Architecture is highlighted by observing current trends in both technology uses and abuses. For example, the number of hosts on the Internet grew from approximately 73 million in 2000 to 440 million in 2006[1]. During that same time frame, the Federally-sponsored Computer Emergency Response Team (CERT) reported the number of vulnerabilities identified and cataloged went from just over 1,000 in 2000 to almost 33,000 in 2006[2]; while information compiled from the FBI and Computer Security Institute[3] indicate that:

- Virus attacks continue to be the source of the greatest financial losses. Unauthorized access continues to be the second-greatest source of financial loss. Financial losses related to laptops (or mobile hardware) and theft of proprietary information (i.e., intellectual property) are third and fourth. These four categories account for more than 74 percent of financial losses.
- Seven percent of respondents thought that insiders account for more than 80 percent of their organization's losses.
- Total losses for 2006 were $52,494,290 for the 313 respondents that were willing and able to estimate losses.

---

[1] "Internet Domain Survey", Internet Software Consortium, January 2007, http://www.isc.org/ds/
[2] "CERT Statistics, 1988-2006", Software Engineering Institute, http://www.cert.org/stats/cert_stats.html
[3] "CSI/FBI Computer Crime and Security Survey", Computer Security Institute, Gordon, L.A., Loeb, M.P., Lucyshyn, W., Richardson, R., 2006. http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf

- Almost 25% of total respondents say that information protection, (i.e., classification, identification and encryption) and application software (Web application) vulnerability security are the most critical issues they face in the next two years.

Three external market factors currently fuel these national trends:

- Latent and immature IT security policy, law and industry standards.
- A shortage of personnel with security technology expertise and experience.
- Engineering for "ease of use" has not been matched by engineering for "ease of secure computing and information sharing".

The Montana Security Architecture, as developed by the CIO's Architecture Team, is a foundational guidance document for addressing these security challenges and technology opportunities, while pursuing the State's business mission. It provides a framework for consistency, coordination, and collaboration in applying security components and controls across Statewide Entities, (SEs).

At the same time, it provides the SE the latitude to use risk-based decision-making processes, i.e., risk management, to determine the appropriate level of protection and product types to be used for obtaining compliance to security policies.

Implementation of the Montana Security Architecture would require the following actions:

1. The formulation and promulgation of Policies, Standards, Procedures, and Guidelines that capture the requirements which are outlined in the Montana Security Architecture.
2. The on-going development and administration of Security Programs by the SE as required by the MCA 2-15-114 http://data.opi.mt.gov/bills/mca/2/15/2-15-114.htm and the Enterprise Information Technology Security Policy as required by http://data.opi.mt.gov/bills/mca/2/17/2-17-534.htm .
3. The review of Information Technology Procurement Requests (ITPRs) submitted by the SE for compliance to the Enterprise Information Technology Security Policy or a planned migration path towards said policy.

4. The creation and staffing of a centralized Office of Enterprise Security (OES) under the direction of the Chief Information Officer (CIO). OES would provide the following administrative services to the SE:

Administrative Service Name	Description
Technology Watch	Stay abreast of new technology and services; and assess, summarize, and report their security impact and value to all SEs.
Best Practices	Stay abreast of new standards, methods, and applications in the industry; and assess, summarize and report successes and best practices to all SEs.
Security Training	Offer training opportunities to the SE to assist them develop their skills sets in such areas as risk assessment, safeguard implementation, incident detection, auditing, etc.
Procurement Contracts	Ascertain the need for state-wide procurement contracts for security products or services, and assess when economies of scale could be achieved.
Collaboration	Establish collaborative relationships with other entities such as law enforcement, public affairs, local governments, universities, and service providers, etc… for rapid response to security issues.
Coordination	Facilitate interactions with both internal and external parties during implementation of security architecture, shared SE projects, and public key infrastructure; and resolve interoperability issues.
Compliance	Create and implement metrics to enable auditing for compliance in establishing, and determining effectiveness, of SE security programs.

5. The creation and staffing of a centralized Network Operations Security Center (NOSC) under the direction of the Deputy Chief Information Officer of Operations (DCIOO). NOSC would provide the following operational services to the SE:

Operational Service Name	Description
Security Consulting	Provide advice to the SE as needed regarding computer security issues for operations.
Incident Response	Establish a network of specialists to assist the SE in containment, eradication, and recovery from security incidents. This team would include staff as well as non-staff members who agree to be "on-call".
Announcements/Alerts	Serve as the focal point for disseminating statewide alerts regarding security threats, active attacks, protective measures, and incident status.
Network Monitoring	Serve as the Enterprise monitoring center for all network traffic on the States infrastructure.
Web Filtering	Serve as the Enterprise Web Filtering center for the State's Internet services.
Host Based Protection	Serve as the Enterprise center for the Host Based solutions that the State provides for all users on the State's network.
PKI Infrastructure	Maintain and manage the PKI infrastructure.

The Architecture Team strongly feels that these actions and related services best position the State to:

- Promote the ease and quality of security engineering across the enterprise.
- Leverage the State's limited resource pool and budget.
- Prevent fragmentation when applying security technology and practices within the SE.
- Allow for the rapid response to both technology opportunities and to security threats.

- Enable the State to take advantage of, adjust to, and/or influence the direction of industry security practices, standards, technology, and legislation.

II. Intent

The intent of the Montana Security Architecture is to provide a framework to enable secure communications and the appropriate level of protection for information resources. This architecture must support the legal requirements established by Federal and State statutes and other mandates pertaining to confidentiality, integrity, availability, and privacy. Within this context, it must also support the secure, efficient transaction of business, delivery of services, and communications with the public, the SE, and businesses. And lastly, it must position the State to be able to quickly respond to technology, business, and information requirement changes without compromising the security, integrity, and performance of the enterprise and its information resources.

III. Introduction and Background

A. Introduction

The Montana Security Architecture is based on a collection of processes taken from Federal Government models, mainly the Federal Information Security Management Act (FISMA) risk management framework (http://csrc.nist.gov/sec-cert/risk-framework.html).

These processes lead to the use of seventeen inter-related security control families developed by the National Institute of Standards and Technology (NIST), and defined in the Federal Information Processing Standards (FIPS) Publication 200 http://csrc.nist.gov/publications/fips/#fips200, (e.g., Access Control, Awareness and Training, Configuration Management, etc.) to develop and implement a comprehensive security program.

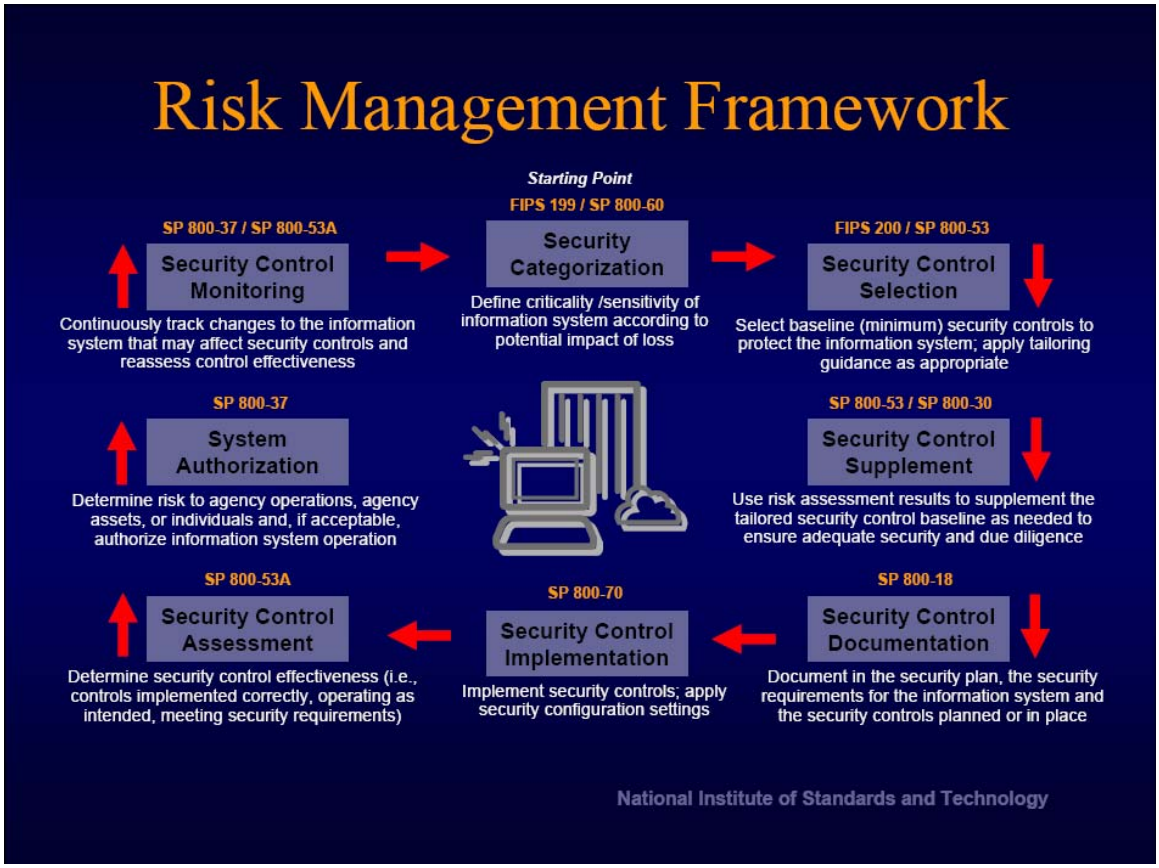

Figure 1 NIST Risk Management Framework

The Risk Management Framework is a methodology developed by NIST to guide the development of an appropriate enterprise security program. The Montana Security Architecture will focus on the Security Control Families as the starting point of our Architecture. The Architecture Team chose to model the Montana

Security Architecture after the Federal Standards for several reasons. One is that by basing the Montana Security Architecture on the FIPS 200 security families the State positions itself to answer any audits from the Federal sector. Another is that by adopting this framework, we gain access to existing methodologies and metrics that are already proven and effective. Lastly and most significantly we establish not only a target security state for Montana that is consistent with recognized national standards but we gain a proven methodology for transitioning from our current security state to our target state.

Following is a list of the 17 security families that comprise our target security state:

1. Risk Assessment
2. Certification, Accreditation and Security Assessments
3. Planning
4. System and Services Acquisition
5. Access Control
6. Identification and Authentication
7. System and Communication Protection
8. Audit and Accountability
9. Awareness and Training
10. Configuration Management
11. Physical and Environmental Protection
12. Personnel Security
13. System and Information Integrity
14. Incident Response
15. Maintenance
16. Contingency Planning
17. Media Protection

For each of these families, a set of security requirements are defined. In this manner, the Montana Security Architecture supports and promotes the consistent and effective development and implementation of security programs by the SE and across the Enterprise.

IV. Methodology

The development of the Montana Security Architecture is part of an overall enterprise architecture. The development of the "Common Requirements Vision" and the "Conceptual Architecture Principles" products were prerequisites to this step in the development process. (The ITSD products can be viewed at: (http://itsd.mt.gov/policy/itpolicy.asp)

The Architecture Team conducted the following four activities as part of the "architecture modeling" of the security architecture:

- Evaluated the implications of the Technology Trends, Enterprise Business Strategies, and Requirements for Technical Architecture from the "ITSD EA Common Requirements Vision" on the security architecture.
- Evaluated the implications of the ITSD Conceptual Architecture Principles (CAP) and then identified any specific domain principles that provide additional structure for the security architecture or which further qualify or contextualize the ITSD CAP from a security perspective.
- Evaluated the security families against the ITSD CAP for support and alignment.
- Identified and established the requirements for the "security families" of the Montana Security Architecture.

V. Principles

These principles represent the fundamental concepts that provide the foundation for the requirements, which compose the Montana Security Architecture.

1. The Architecture Team endorses and supports the ITSD CAP, and deems them applicable to the Montana Security Architecture as qualified in Item 2 below.
2. The Architecture Team has further identified the following domain specific principles, which provide additional structure for the Montana Security Architecture, and which further qualify and/or contextualize the ITSD CAP from a security perspective.
3. The security architecture must facilitate proper and efficient security identification, authentication, authorization, administration and auditability in response to the access and use of information resources.
4. The security architecture must support and remain compliant with State laws and Federal regulations with respect to security, privacy, availability, accessibility, etc.
5. The security architecture must provide a modular approach to authentication, authorization, and accounting.

6. The security architecture must provide for portability across platforms.
7. The security architecture must utilize Open Standards wherever possible at all modular levels.
8. The security architecture must support multiple service delivery channels where feasible.
9. The security architecture must be flexible and adaptable enough to support the introduction and/or integration of new technologies, while maintaining appropriate security protection and requirements.
10. The security architecture must ensure that the accountability and responsibility of all persons fulfilling security duties are sustainable, assignable, and enforceable.
11. The security architecture must address systemic needs as well as individual component needs.
12. The security architecture must address and support multiple levels of protection, including network level, operating system, and application level security needs.
13. The security architecture must facilitate and encourage a risk management approach to security.

VI. Security Families

The following seventeen security control families are integral to the security architecture. All the families fall into one of three general classes, Managerial, Technical and Operational. Managerial controls are those security controls that focus on the management of risk and information system security. Technical controls are those security controls that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. Operational controls are those security controls that are primarily implemented and executed by people as opposed to systems.

Managerial	Technical	Operational
Risk Assessment	Access Control	Awareness and Training
Certification, Accreditation and Security Assessments	Identification and Authentication	Configuration Management
Planning	System and Communication Protection	Physical and Environmental Protection
System Services Acquisition	Audit and Accountability	Personnel Security
		System and Information Integrity
		Incident Response
		Maintenance
		Contingency Planning
		Media Protection

A. Managerial Class

1. Risk Assessment

The SE must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

2. Certification, Accreditation and Security Assessments

The SE must:

a. periodically assess the security controls in organizational information systems to determine if the controls are effective in their application;

b. develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems;

c. authorize the operation of organizational information systems and any associated information system connections; and

d. monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

3. Planning

The SE must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

4. System and Services Acquisition

The SE must:

a. allocate sufficient resources to adequately protect organizational information systems;

b. employ system development life cycle processes that incorporate information security considerations;

c. employ software usage and installation restrictions; and

d. ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

B. Technical Class

5. Access Control

The SE must; limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

6. Identification and Authentication

The SE must; identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

7. System and Communication Protection

The SE must:

a. monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and

b. employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

8. Audit and Accountability

The SE must:

a. create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and

b. ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

C. Operational Class

9. Awareness and Training

The SE must:

a. ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, mandates, directives, policies, standards, instructions,

regulations, or procedures related to the security of organizational information systems; and

b. ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

10. Configuration Management

The SE must:

a. establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and

b. establish and enforce security configuration settings for information technology products employed in organizational information systems.

11. Physical and Environmental Protection

The SE must;

a. limit physical access to information systems, equipment, and the respective operating environments to authorized individuals;

b. protect the physical plant and support infrastructure for information systems;

c. provide supporting utilities for information systems;

d. protect information systems against environmental hazards; and

e. provide appropriate environmental controls in facilities containing information systems.

12. Personnel Security

The SE must:

a. ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions;

b. ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and

c. employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

13. System and Information Integrity

The SE must:

a. identify, report, and correct information and information system flaws in a timely manner;

b. provide protection from malicious code at appropriate locations within organizational information systems; and

c. monitor information system security alerts and advisories and take appropriate actions in response.

14. Incident Response

The SE must:

a. establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and

b. track, document, and report incidents to appropriate organizational officials and/or authorities.

15. Maintenance

The SE must:

a. perform periodic and timely maintenance on organizational information systems; and

b. provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

16. Contingency Planning

The SE must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

17. Media Protection

The SE must:

a. protect information system media, both paper and digital;

b. limit access to information on information system media to authorized users; and

c. sanitize or destroy information system media before disposal or release for reuse.

VII. Risk Assessment

The SE must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

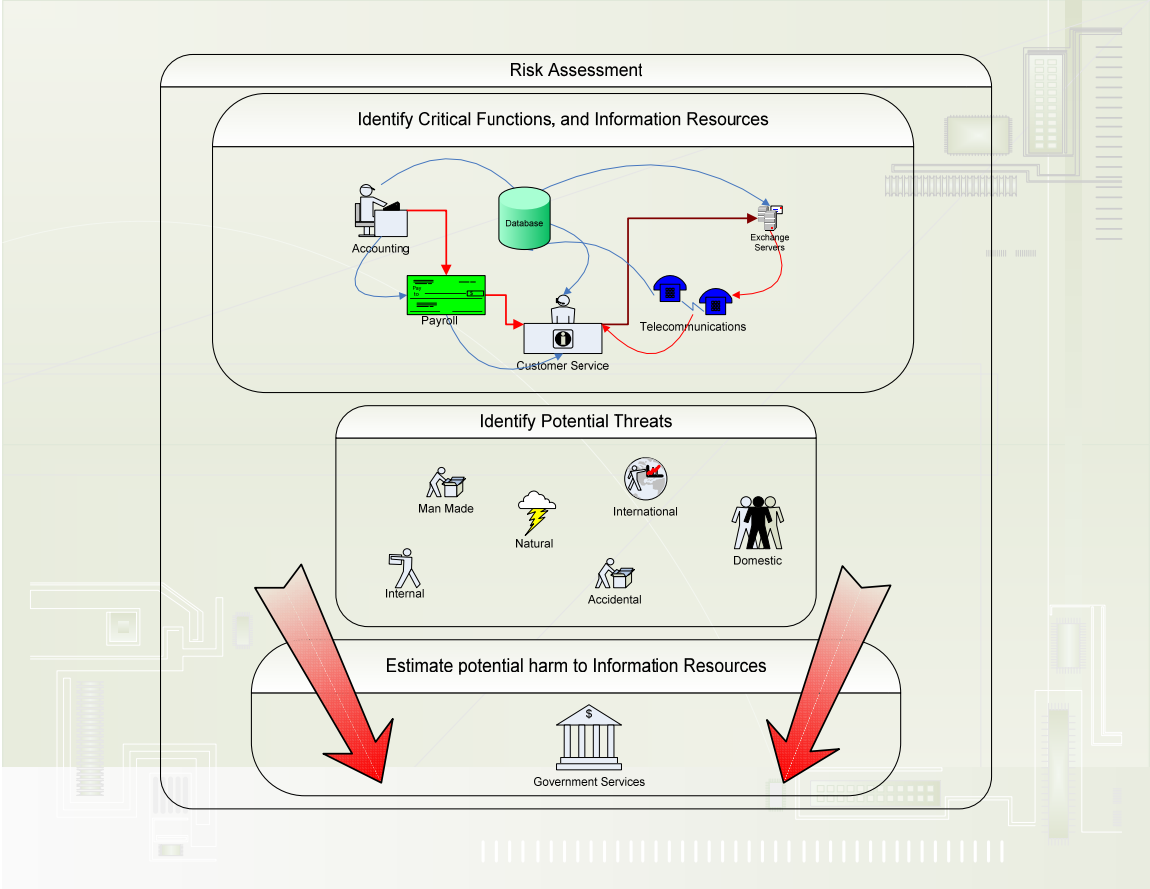

Figure 2 Risk Assessment

Risk Assessment refers to those practices, technologies and/or services used to identify information resources that are confidential and/or critical to the SE; and to identify and evaluate the potential security threats, and associated risks, to those resources.

The starting point of establishing effective information technology security is to identify the information resources that are owned and/or utilized by the SE. “Information resources” include government information, information technology, and associated personnel.

Once the level of criticality and/or sensitivity of the information resources have been identified through the business impact analysis, the threats to which they are subject need to be evaluated. This process is referred to as risk management. The probability of each "threat event" occurring and the resultant impact of that event on the information resources are assessed during this process.

Examples of potential impacts that would adversely affect the SE's mission, functions, image or reputation include financial loss, public embarrassment, loss of public confidence, trust, noncompliance to State or Federal statutes and other mandates, and degraded customer (public) service.

During the risk management process, the SE determines what types of controls are appropriate to address their defined risks. In this manner, the controls deployed reflect the true importance of the SE's investment in the information resources used to accomplish the SE's mission.

Risk management is the process of managing risks to operations of an information system which includes the following components:

- the performance of a risk assessment;
- the implementation of a risk management strategy;
- employment of techniques and procedures for the continuous monitoring of the security state of the information system.

Risk management should not be viewed as just a one-time task or project, but rather as a tactical operational process. Both internal changes (e.g., changes to technical infrastructure or to applications) as well as external changes (e.g., technology advances, new Federal statutes, etc.) could directly impact the level of sensitivity and the threats applicable to information resources. The SE, therefore, should intermittently deploy risk assessment and risk management techniques to determine if their security controls are relevant and adequate, and then update their controls accordingly.

Requirements

RA-1 The SE develops, disseminates, and periodically reviews/updates:

1. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

RA-2	The SE categorizes the information system and the information processed, stored, or transmitted by the system in accordance with applicable laws, mandates, directives, policies, regulations, standards, and guidance; and then documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations.
RA-3	The SE conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the SE (including information and information systems managed/operated by external parties).
RA-4	The SE updates the risk assessment periodically *[organization-defined frequency, at least annually]* or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.
RA-5	The SE scans for vulnerabilities in the information system periodically *[organization-defined frequency, at least quarterly]* or when significant new vulnerabilities potentially affecting the system are identified and reported.

VIII. Certification, Accreditation and Security Assessments

The SE must:

1. Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application;
2. develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems;
3. authorize the operation of organizational information systems and any associated information system connections; and
4. monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Certification refers to a comprehensive assessment of the managerial, technical, and operational security controls in an information system made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system.

The certification documentation is then presented to a senior management individual in the SE for accreditation. Accreditation is the formal decision by senior management authorizing the operation of an information system and to explicitly accept risks to SE operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

The certification documentation and accreditation document become what is known as a C&A package.

Requirements

CA-1 The SE develops, disseminates, and periodically reviews/updates:

1. Formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.

CA-2 The SE conducts an assessment of the security controls in the information system [*organization-defined frequency, at least annually*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

CA-3 The SE authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.

CA-4 The SE conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

CA-5 The SE develops and updates [*organization-defined frequency*], a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

CA-6	The SE authorizes (i.e., accredits) the information system for processing before -operations and updates the authorization [*organization-defined frequency, at least every three years*] or when there is a significant change to the system. A senior organizational official signs and approves the security accreditation.
CA-7	The SE monitors the security controls in the information system on an ongoing basis.

IX. Planning

The SE must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

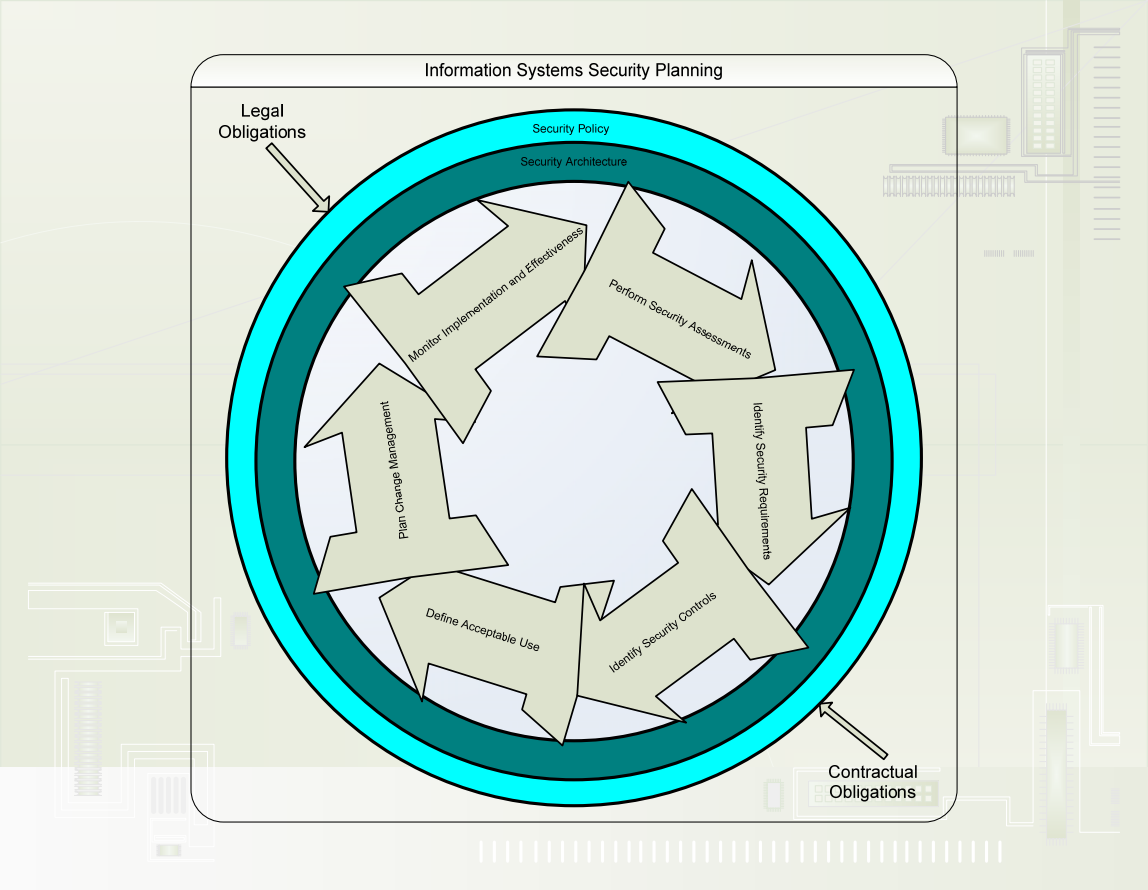

Figure 3 Information Systems Security Planning

The Systems Security Plan is a formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. The plan must be aligned with the enterprise architectures and in compliance with the security policy.

Included in the plan are routine security-related activities; security assessments, audits, system hardware and software maintenance, security certifications and testing/exercises, etc. The plan should contain both emergency and routine situations.

Requirements

PL-1 The SE develops, disseminates, and periodically reviews/updates:

1. A formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

PL-2 The SE develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.

PL-3 The SE reviews the security plan for the information system [*organization-defined frequency, at least annually*] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.

PL-4 The SE establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

PL-5 The SE plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

PL-6 The SE conducts a privacy impact assessment on the information system in accordance with legal or contractual requirements.

X. System and Services Acquisition

The SE must:

1. Allocate sufficient resources to adequately protect organizational information systems;
2. employ system development life cycle processes that incorporate information security considerations;
3. employ software usage and installation restrictions; and
4. ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

System and Services Acquisition deals with ensuring that the systems and services that are developed and/or procured, are secured in a manner that is consistent with its categorization. This control ensures that security is part of the entire system development lifecycle to include documenting of security requirements during the analysis phase. Included is management's commitment to ensure resources can be obtained to adequately secure the systems/or services through the end of the lifecycle. The requirements contained in the documentation for the development must be followed.

The SE must protect the end device by ensuring that software restrictions can be placed on the clients to allow only approved software thereby ensuring the security of the entire system.

Requirements

SA-1 The SE develops, disseminates, and periodically reviews/updates:

1. A formal, documented, system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

SA-2 The SE determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system.

SA-3 The SE manages the information system using a system development

	life cycle methodology that includes information security considerations.
SA-4	The SE includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, mandates, directives, policies, regulations, and standards.
SA-5	The SE obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.
SA-6	The SE complies with software usage restrictions.
SA-7	The SE enforces explicit rules governing the installation of software by users.
SA-8	The SE designs and implements the information system using security engineering principles such as the NIST Risk Management Framework.
SA-9	The SE: **1.** Requires that providers of external information system services employ adequate security controls in accordance with applicable laws, mandates, directives, policies, regulations, standards, guidance, and established service-level agreements; and **2.** monitors security control compliance.
SA-10	The SE requires that information system developers create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.
SA-11	The SE requires that information system developers create a security test and evaluation plan, implement the plan, and document the results.

XI. Access Control

The SE must; limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

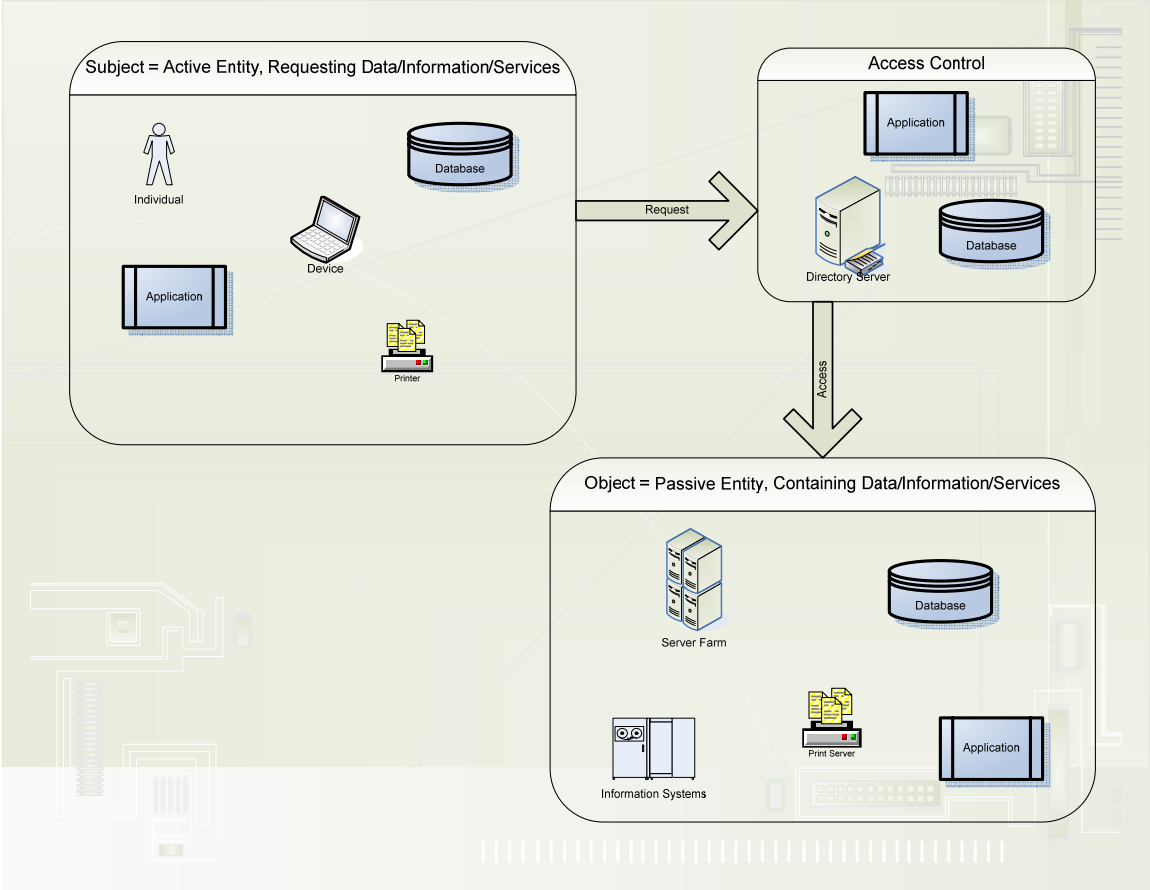

Figure 4 Access Control

Access control is the technical control that ensures that an individual, process, or other device only has access to the information system for which they have been authorized. This prevents the individual, process, or other device from obtaining, adding, or modifying information for which they do not have authorization or a need to know. This helps prevent information disclosure and corruption of data.

Requirements

AC-1 The SE develops, disseminates, and periodically reviews/updates:

1. A formal, documented, access control policy that addresses purpose, scope, roles, responsibilities,

	management commitment, coordination among organizational entities, and compliance; and **2.** formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.
AC-2	The SE manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [*organization -defined frequency, at least annually*].
AC-3	The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.
AC-4	The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.
AC-5	The information system enforces separation of duties through assigned access authorizations.
AC-6	The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.
AC-7	The information system enforces a limit of [*organization-defined number*] consecutive invalid access attempts by a user during a [*organization-defined time period*] time period. The information system automatically [*locks the account/node for an* [*organization-defined time period*], *delays next login prompt according to organization-defined delay algorithm.*]], when the maximum number of unsuccessful attempts is exceeded.
AC-8	The information system displays an approved, system use notification message before granting system access informing potential users: **1.** that the user is accessing a Government information system; **2.** that system usage may be monitored, recorded, and subject to audit; **3.** that unauthorized use of the system is prohibited and subject to criminal and civil penalties; **4.** that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions

	to log on to the information system; **5.** if any Federal or State statute or other mandate requires additional components in the banner those requirements must also be met.
AC-9	The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.
AC-10	The information system limits the number of concurrent sessions for any user to [*organization-defined number of sessions*].
AC-11	The information system prevents further access to the system by initiating a session lock after [*organization-defined time period*] of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.
AC-12	The information system automatically terminates a remote session after [*organization-defined time period*] of inactivity.
AC-13	The SE continuously supervises and reviews [*organization-defined frequency, at least quarterly]* the activities of users with respect to the enforcement and usage of information system access controls consummate with the sensitivity of the information system.
AC-14	The SE identifies and documents specific user actions that can be performed on the information system without identification or authentication.
AC-15	The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions*.*
AC-16	The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions*.*
AC-17	The SE authorizes, monitors, and controls all methods of remote access to the information system.
AC-18	The SE: **1.** Establishes usage restrictions and implementation guidance for wireless technologies; and **2.** authorizes, monitors, controls wireless access to the information system.

AC-19 The SE:

1. Establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and
2. authorizes, monitors, and controls device access to organizational information systems.

AC-20 The SE establishes terms and conditions for authorized individuals to:

1. Access the information system from an external information system; and
2. process, store, and/or transmit organization-controlled information using an external information system.

XII. Identification and Authentication

The SE must; identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems

Authentication refers to the process of verifying the identity of a user. Authorization refers to the process of establishing and enforcing a user's rights and privileges to access specified resources. Encryption refers to the cryptographic transformation of data to render it unintelligible through an algorithmic process using a cryptographic key, so that it can be reconverted only by an authorized recipient holding the matching key.

Authentication answers the question, "Are you who you say you are?" It is a means of establishing the validity of a claimed identity to the system, which becomes the basis for individual accountability. There are three means of authenticating a user's identity, which can be used alone or in combination:

1. Validating something the individual knows (e.g., a password, a Personal Identification Number (PIN), or a cryptographic key);
2. validating something the individual possesses, referred to as a "token" (e.g., an ATM card or a smart card); or
3. validating something the individual "is", referred to as a "biometric" (e.g., fingerprints or voice patterns).

Two factor authentication refers to when two or more different means are used together to validate an identity.

Once authenticated, logical access controls are utilized to authorize and enforce a user's access to and actions towards specified resources. This authorization may be based on identity, roles (e.g., data entry clerk, administrator, supervisor), location, time, types of transactions, service constraints (e.g., number of concurrent users), access mode (e.g., read, write, delete), or a combination of these criteria.

Both internal authorization controls (such as Access Control Lists) and external controls (such as secure gateways/firewalls) can be deployed. Another mechanism that can be used for strong access control is encryption, whereby encrypted information can only be decrypted by those possessing the appropriate cryptographic key. For example: Advanced Encryption Standard (AES).

Requirements

IA-1 The SE develops, disseminates, and periodically reviews/updates:

1. A formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

IA-2 The information system uniquely identifies and authenticates users (or processes acting on behalf of users).

IA-3 The information system identifies and authenticates specific devices before establishing a connection.

IA-4 The SE manages user identifiers by:

1. Uniquely identifying each user;
2. verifying the identity of each user;
3. receiving authorization to issue a user identifier from an appropriate organization official;
4. issuing the user identifier to the intended party;
5. disabling the user identifier after [*organization-defined time period*] of inactivity; and (vi) archiving user identifiers.

IA-5 The SE manages information system authenticators by:

	1. Defining initial authenticator content; **2.** establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; **3.** changing default authenticators upon information system installation; and **4.** changing/refreshing authenticators periodically.
IA-6	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
IA-7	The information system employs authentication methods that meet the requirements of applicable laws, mandates, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

XIII. System and Communications Protection

The SE must:

1. Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and
2. employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

System and Communication Protection refers to those practices, technologies and/or services used to protect, identify, and deter attacks from internal and external sources though Defense in Depth. Defense in Depth is the practice of layering security so that if even one defense is broken others will still protect the information asset. Included in the System and Communications Protection family are desktop protections such as end point security, anti-malware software, host intrusion detection/prevention, firewalls, etc. This could also include encryption and disposal of information.

On the server side, requirements such as ensuring that applications and critical or sensitive data are separated, resources can be prioritized, management of the system and use of the system are separated.

Network protections include requirements such as compartmentalization, which means groupings of systems are logically separated and can only be joined by explicit means. Other protections include requirements for encryption as traffic

passes over the network as well as ensuring traffic follows a known trusted path. This is accomplished by means of verifying authenticity of routers and their associated routing protocols.

The network and systems must be resilient to denial of service attacks and use cryptography when needed.

Requirements

SC-1 The SE develops, disseminates, and periodically reviews/updates:

1. A formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

SC-2 The information system separates user functionality (including user interface services) from information system management functionality.

SC-3 The information system isolates security functions from non-security functions.

SC-4 The information system prevents unauthorized and unintended information transfer via shared system resources.

SC-5 The information system protects against or limits the effects of the following types of denial of service attacks: [*organization-defined list of types of denial of service attacks or reference to source for current list*].

SC-6 The information system limits the use of resources by priority.

SC-7 The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

SC-8 The information system protects the integrity of transmitted information.

SC-9 The information system protects the confidentiality of transmitted information.

SC-10 The information system terminates a network connection at the end of a session or after [*organization-defined time period*] of inactivity.

SC-11	The information system establishes a trusted communications path between the user and the following security functions of the system: *[organization-defined security functions to include at a minimum, information system authentication and re-authentication]*.
SC-12	When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.
SC-13	For information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, mandates, directives, policies, regulations, standards, and guidance.
SC-14	The information system protects the integrity and availability of publicly available information and applications.
SC-15	The information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.
SC-16	The information system reliably associates security parameters with information exchanged between information systems.
SC-17	The SE issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.
SC-18	The organization: **1.** Establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and **2.** authorizes, monitors, and controls the use of mobile code within the information system.
SC-19	The SE: **1.** Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and **2.** authorizes, monitors, and controls the use of VoIP within the information system.

SC-20	The information system that provides name/address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries.
SC-21	The information system that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.
SC-22	The information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation.
SC-23	The information system provides mechanisms to protect the authenticity of communications sessions.

XIV. Audit and Accountability

The SE must:

1. Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and
2. ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Auditing System Activities refers to those practices, technologies and/or services used to ensure that the implementation and maintenance of security controls and system changes are adequately documented and managed, such that accountability can be established.

Auditing System Activities provide a means to access policy compliance (e.g., security check list), verify operational assurance (e.g., penetration testing), maintain individual accountability (e.g., user audit trails, change management approvals), and to support intrusion problem analysis (e.g., user behavior anomalies; repeated failed log- in attempts; reconstruction of events).

Auditing System Activities can be self-administered (by the SE) or independently administered (by parties external to the SE). Personnel involved in these activities must have a high-level of expertise in the information technology security field and of auditing practices; and must administer said activities objectively.

Industry studies suggest that security controls tend to degrade over the operational lifecycle of systems as users and operators discover new ways to intentionally or unintentionally bypass or subvert security. The SE must therefore make a risk-based decision regarding the timing (e.g., annual independent audit; daily audit log analysis) and scope (e.g., system, application or user level) of Auditing System Activities.

Requirements

AU-1 The SE develops, disseminates, and periodically reviews/updates:

1. A formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

AU-2 The information system generates audit records for the following events: [*organization-defined auditable events*].

AU-3 The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

AU-4 The SE allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

AU-5 The information system alerts appropriate organizational officials in the event of an audit processing failure and takes the following additional actions: [*organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

AU-6 The SE regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

AU-7 The information system provides an audit reduction and report generation capability.

AU-8 The information system provides time stamps for use in audit record generation.

AU-9 The information system protects audit information and audit tools from

	unauthorized access, modification, and deletion.
AU-10	The information system provides the capability to determine whether a given individual took a particular action.
AU-11	The SE retains audit records for [*organization-defined time period*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

XV. Awareness and Training

The SE must:

1. Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, mandates, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and
2. ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Security Awareness refers to those practices, technologies and/or services used to promote user awareness, training, and responsibility with regards to security risks, vulnerabilities, methods, and procedures related to information technology resources.

A “user” is an individual or group who has access to an information system and/or its data. Users within an SE need to understand the sensitivity of the SE’s information resources (See “Risk Assessment”) and their responsibility in protecting those resources.

For example, users should be, at a minimum, aware of the threats and the associated impacts of a compromised password; potential viruses transmitted over the Internet; corrupted databases; and of the accessibility of printed information generated from the system.

Upon engagement, users are responsible to adhere to Federal and State statutes or other mandates and SE policy and procedures. Security Awareness programs provide a proactive mechanism to foster further comprehension of an individual’s security responsibilities; to contextualize security responsibilities to specific job duties and case examples; to motivate personnel towards a security-conscious behavior while performing their duties; and to reinforce the consequences of security failures on the State, the SE, its mission, its customers, and the user.

The appropriate amount, depth, and timing of Security Awareness training is a risk-based decision. Best practices suggest that a Security Awareness program that utilizes a combination of periodic training sessions (introductory/refresher) and on-going security awareness promotion (marketing) are most effective. In addition, where appropriate, an SE may decide not to grant certain access rights to personnel until the desired level of Security Awareness Training has been successfully completed.

Lastly, as the business and technical environment changes, security awareness material will need to be updated accordingly.

For those responsible for assuring security of an SE's information assets, security awareness training refers to those practices, technologies and/or services used in training Information Security Officers (ISO), system administrators and/or other personnel involved in the administration or development of information systems. Individuals who are assigned responsibilities for information technology security controls need in-depth training regarding the security methodologies and techniques required to develop, configure, implement, administer, and maintain those controls.

For example, a security administrator may need to know the method and techniques for granting various types of access rights to the database, how to set up and maintain an effective firewall to filter external access, and how to detect intrusions to the system. Typical sources for technical training include instructor-led programs (3rd party or internal), commercial off the-shelf training modules, technical publications, and operations manuals provided by the vendor and may include security certifications.

Requirements

AT-1 The SE develops, disseminates, and periodically reviews/updates:

1. A formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

AT-2 The SE provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and [*organization-defined frequency, at least annually*] thereafter.

AT-3 The SE identifies personnel that have significant information system

	security roles and responsibilities during the system development life cycle, documents those roles and responsibilities, and provides appropriate information system security training: **1.** Before authorizing access to the system or performing assigned duties; **2.** when required by system changes; and **3.** [*organization-defined frequency*] thereafter.
AT-4	The SE documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.
AT-5	The SE establishes and maintains contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations to stay up to date with the latest recommended security practices, techniques, and technologies and to share the latest security-related information including threats, vulnerabilities, and incidents.

XVI. Configuration Management

The SE must:

1. Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and
2. establish and enforce security configuration settings for information technology products employed in organizational information systems.

Configuration Management activities refer to those practices, technologies and/or services that create a trusted environment for the information system. The basis of any configuration management activity is to determine a baseline configuration for all information systems. This is where the configuration settings and component inventories will be documented. These documents should also include network diagrams.

These documents become important in troubleshooting strange behaviors, setup the ability to track metrics over time for capacity planning, as well as provide a basis for disaster recovery among other advantages.

For systems categorized as having higher criticality and/or sensitivity, configuration management includes change control, monitoring change, and access restrictions for those changes. Included in the higher categories, the

principle of least functionality comes into play. This means that an information system is configured with only the requirements needed to support the operation of that system.

For example, if an information system requires a web server, and the server is also configured as a file transfer, domain name, and an application server the principle of least functionality is not being followed. In this example, any of the additional functions could allow for an attacker to compromise the criticality and/or the sensitivity of the system.

Requirements

CM-1 The SE develops, disseminates, and periodically reviews/updates:

1. A formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

CM-2 The SE develops, documents, and maintains a current baseline configuration of the information system.

CM-3 The SE authorizes, documents, and controls changes to the information system.

CM-4 The SE monitors changes to the information system conducting security impact analyses to determine the effects of the changes.

CM-5 The SE:

1. Approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and
2. generates, retains, and reviews records reflecting all such changes.

CM-6 The SE:

1. Establishes mandatory configuration settings for information technology products employed within the information system;
2. configures the security settings of information technology products to the most restrictive mode consistent with

	operational requirements; **3.** documents the configuration settings; and **4.** enforces the configuration settings in all components of the information system.
CM-7	The SE configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: [*organization-defined list of prohibited and/or restricted functions, ports, protocols, and/or services*].
CM-8	The SE develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information.

XVII. Physical Security

The SE must:

1. Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals;
2. protect the physical plant and support infrastructure for information systems;
3. provide supporting utilities for information systems;
4. protect information systems against environmental hazards; and
5. provide appropriate environmental controls in facilities containing information systems.

Physical Security refers to those practices, technologies and/or services used to ensure that physical security controls are applied. Physical security controls take into account 1) the physical facility housing the information resources; 2) the general operating location; and 3) the support facilities that underpin the operation of the information systems.

Accordingly, physical security controls need to be considered for information resources residing in static facilities (such as buildings), mobile facilities (such as computers mounted in vehicles), and portable facilities (in-transit facility housing). Appropriate physical controls need to be established based on the risks related to geographic location, including natural threats (such as flooding), man-made threats (such as burglary or civil disorders), and threats from nearby activities (such as toxic chemical processing or electromagnetic interference). Lastly, physical controls need to assure that the appropriate levels of support facilities such as electric power, heating, water, and air-conditioning are sustainable as required by the information resources.

For example, physical access controls may be used to restrict and monitor the entry and exit of personnel to/from a room, a data center, or a building. Physical access controls may range from badges and locks to retina scanning personal identification devices and vibration detectors. Physical access controls should be considered for those areas containing system hardware, as well as for those areas which house network wiring, electric power, backup media, source documents, etc.

Physical security controls provide a first line of defense for information resources against physical damage, physical theft, unauthorized disclosure of information, loss of control over system integrity, and interruption to computer services. Physical security is also a critical component of the Defense in Depth philosophy.

Requirements

PE-1 The SE develops, disseminates, and periodically reviews/updates:

1. A formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

PE-2 The SE develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials. Designated officials within the organization review and approve the access list and authorization credentials [*organization-defined frequency, at least annually*].

PE-3 The SE controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

PE-4 The SE controls physical access to information system distribution and transmission lines within organizational facilities.

PE-5 The SE controls physical access to information system devices that display information to prevent unauthorized individuals from observing

	the display output.
PE-6	The SE monitors physical access to the information system to detect and respond to physical security incidents.
PE-7	The SE controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.
PE-8	The SE maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: **1.** Name and organization of the person visiting; **2.** signature of the visitor; **3.** form of identification; **4.** date of access; **5.** time of entry and departure; **6.** purpose of visit; and **7.** name and organization of person visited. Designated officials within the organization review the visitor access records [*organization-defined frequency*].
PE-9	The SE protects power equipment and power cabling for the information system from damage and destruction.
PE-10	The SE provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.
PE-11	The SE provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.
PE-12	The SE employs and maintains automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes.
PE-13	The SE employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.

PE-14	The SE regularly maintains, within acceptable levels, and monitors the temperature and humidity within the facility where the information system resides.
PE-15	The SE protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.
PE-16	The SE authorizes and controls information system-related items entering and exiting the facility and maintains appropriate records of those items.
PE-17	The SE employs appropriate management, operational, and technical information system security controls at alternate work sites.
PE-18	The SE positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.
PE-19	The SE protects the information system from information leakage due to electromagnetic signals emanations.

XVIII. Personnel Security

The SE must:

1. Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions;
2. ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and
3. employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

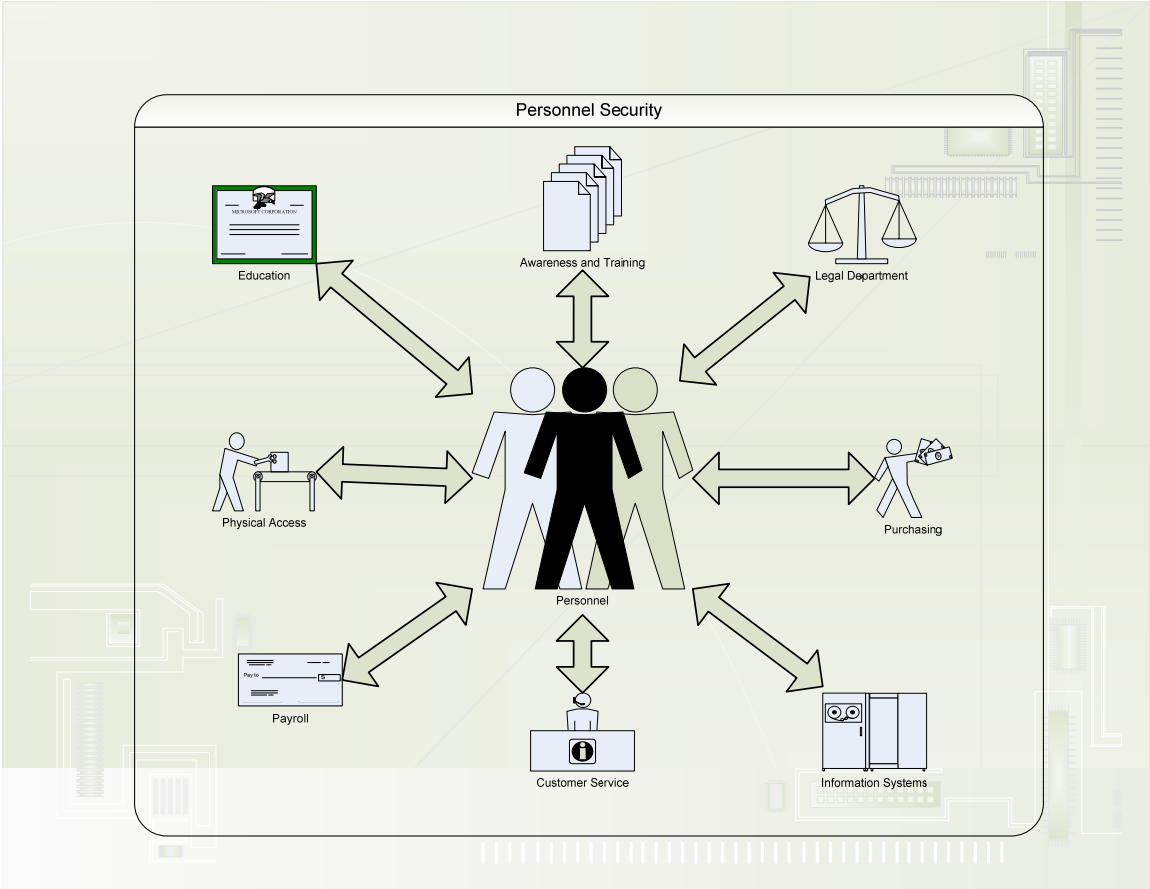

Figure 5 Personnel Security

Personnel Security refers to those practices, technologies and/or services used to ensure that personnel security controls are applied appropriately to those personnel working for, or on behalf, of the SE.

Personnel Security begins during the staffing process. Early in the process of defining a position, the responsible supervisor determines the type of computer access that is needed for the position and the sensitivity of that position. Best practices suggest that two general principles should be followed in defining a position: separation of duties and least privilege. Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process.

For example, separate responsibility should be given for requesting a personal identification number and for authorizing a personal identification number. Least privilege refers to granting a user only those accesses that they need to perform their official duties.

For example, a data entry clerk may not need to run analysis reports against the entire SE database. As part of the process to fill a position, best practices also

suggest that testing and background screening should be used as appropriate to help validate and/or access a candidate's qualifications, past performance and appropriateness for a particular position.

Personnel security controls are administered according to the SE's security policy via user account management. User account management involves

1. Establishing the procedures for requesting, issuing, and closing user accounts over the life cycle events of personnel (e.g., initial hire, transfers, position authorizations); and
2. managing these functions on an on-going basis.

Requirements

PS-1 The SE develops, disseminates, and periodically reviews/updates:

1. A formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

PS-2 The SE assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations [*organization-defined frequency*].

PS-3 The SE screens individuals requiring access to organizational information and information systems before authorizing access.

PS-4 The SE, upon termination of individual employment, terminates information system access, conducts exit interviews, retrieves all organizational information system-related property, and provides appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems.

PS-5 The SE reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization and initiates appropriate actions.

PS-6 The SE completes appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access and reviews/updates the agreements

	[*organization-defined frequency*].
PS-7	The SE establishes personnel security requirements including security roles and responsibilities for third-party providers and monitors provider compliance.
PS-8	The SE employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

XIX. System and Information Integrity

The SE must:

1. Identify, report, and correct information and information system flaws in a timely manner;
2. provide protection from malicious code at appropriate locations within organizational information systems; and
3. monitor information system security alerts and advisories and take appropriate actions in response.

System and Information Integrity refer to those practices, technologies and/or services used to ensure the integrity of the data in the SE's systems. This includes detection of flaws and vulnerabilities in applications as well as systems. It also addresses patching of those applications and systems. Antivirus and Anti-malware solutions would be included in these safeguards. The methods and tools used to monitor and detect anomalies on the SE's network are also critical to system and information integrity.

In addition to the communications inherent in Security Awareness and Technical Training, the security architecture requires a means to support the timely and meaningful exchange of information regarding:

1. New security technology products and/or features, best practices, emerging industry standards, and security controls success stories;
2. proposed changes to the security infrastructure and associated implementation plans; and
3. alerts, status, and recommended actions in response to security attacks.

Examples of technical communication medium include internal enterprise list servers, government sponsored security conferences, subscriptions to security research consortiums, etc.

Technical communications are instrumental in the security architecture as they foster both a proactive stance and a systemic view in addressing security issues within a dynamic business and technology environment.

Requirements

SI-1 The SE develops, disseminates, and periodically reviews/updates:

1. A formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

SI-2 The SE identifies, reports, and corrects information system flaws.

SI-3 The information system implements malicious code protection.

SI-4 The SE employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.

SI-5 The SE receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.

SI-6 The information system verifies the correct operation of security functions [*Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every* [*organization-defined time-period*]] and [*Selection (one or more): notifies system administrator, shuts the system down, restarts the system*] when anomalies are discovered.

SI-7 Where necessary the information system detects and protects against unauthorized changes to software and information.

SI-8 The information system implements spam protection.

SI-9 The SE restricts the capability to input information to the information system to authorized personnel.

SI-10 The information system checks information for accuracy, completeness, validity, and authenticity.

SI-11 The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.

SI-12 The SE handles and retains output from the information system in accordance with applicable laws, mandates, directives, policies, regulations, standards, and operational requirements.

XX. Incident Response

The SE must:

1. Establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and
2. track, document, and report incidents to appropriate organizational officials and/or authorities.

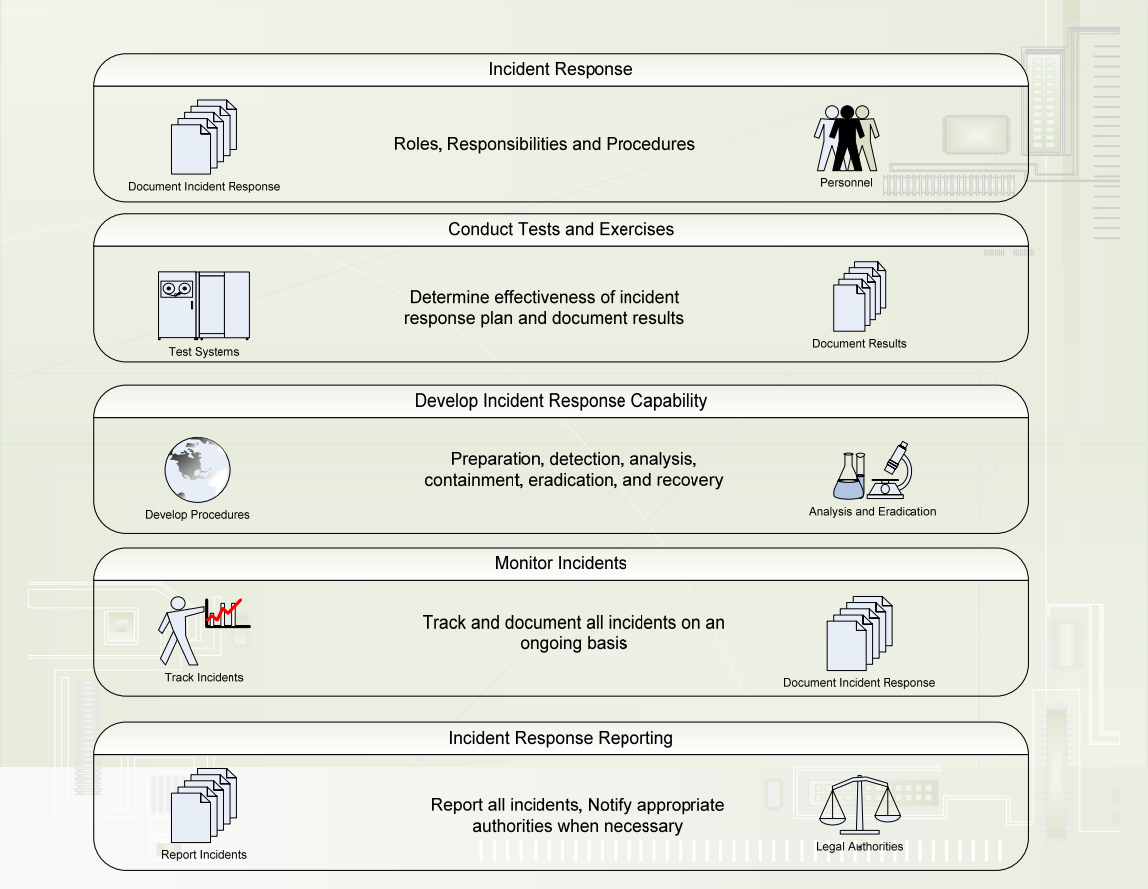

Figure 6 Incident Response

Incident Response refers to those practices, technologies and/or services used to respond to suspected or known incidents. Once an incident has been detected it is imperative that the incident be assessed as soon as possible so

that the proper response can be determined according the SE's policies and procedures, so that any further damage and risk exposure to the SE and the State are avoided or minimized. Information technology security incidents refer to both intentional and unintentional events which may be technical (e.g., viruses, system hacking, mis-configuration) or non-technical (e.g., theft, property abuse, service disruption). If the incident is not responded to in a timely manner, the damage resulting from an incident could spread within, and/or across SEs.

Handling incidents can be logistically complex, and may require information and assistance from sources outside the SE (e.g., technical specialists, the FBI, First Responders, or the public information office). Industry best practices suggest that organizations who adopt both proactive and reactive means to address incident handling are better able to limit the negative implications of incidents.

Examples of proactive activities include establishing communication mechanisms to report incidents and to disseminate incident alerts; and identifying technical experts who can provide emergency assistance if needed. Examples of reactive activity include blocking or aborting computer processes; temporarily denying user access; and deploying inoculation software.

Requirements

IR-1 The SE develops, disseminates, and periodically reviews/updates:

1. A formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

IR-2 The SE trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training [*organization-defined frequency, at least annually*].

IR-3 The SE tests and/or exercises the incident response capability for the information system [*organization-defined frequency, at least annually*] using [*organization-defined tests and/or exercises*] to determine the incident response effectiveness and documents the results.

IR-4 The SE implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

IR-5 The SE tracks and documents information system security incidents on

	an ongoing basis.
IR-6	The SE promptly reports incident information to appropriate authorities.
IR-7	The SE provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the SE's incident response capability.

XXI. Maintenance

The SE must:

1. Perform periodic and timely maintenance on organizational information systems; and
2. provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

The maintenance operations control refers to those practices, technologies and/or services used to; respond to, document, and manage, the maintenance of the SE's information systems. This area focuses on monitoring systems and completing routine maintenance tasks such as ensuring that software and firmware are up to date with the most current feasible software release.

There should be a policy specifying which systems have support from third parties. If no third party support is contracted, a minimal set of replacement equipment must be available on site. This is all dependent on the criticality of the information system. The more critical a system is, the shorter the response time should be for support by either the internal organization or the contracted third party(s).

This control also looks at how the systems are to be monitored and maintained. For instance, one of the requirements is that all remotely executed maintenance is closely monitored by the SE to ensure that only authorized and approved maintenance is taking place.

Requirements

MA-1	The SE develops, disseminates, and periodically reviews/updates: **1.** A formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **2.** formal, documented procedures to facilitate the

	implementation of the information system maintenance policy and associated system maintenance controls.
MA-2	The SE schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.
MA-3	The SE approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.
MA-4	The SE authorizes, monitors, and controls any remotely executed maintenance and diagnostic activities, if employed.
MA-5	The SE allows only authorized personnel to perform maintenance on the information system.
MA-6	The SE obtains maintenance support and spare parts for [*organization-defined list of key information system components*] within [*organization-defined time period*] of failure.

XXII. Contingency Planning

The SE must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Contingency planning refers to those practices, technologies and/or services used to respond to emergencies, restore operations, and provide for post-disaster recovery of SE systems based on the criticality and sensitivity of the information system.

Contingency planning is the process by which plans are developed and documented to provide for efficient restoration of critical systems in a timely and organized manner. Once the initial planning is complete, those plans should be tested in accordance with SE developed policy to ensure the accuracy and usability of the plans. Any deficiencies that are noted during testing should be immediately documented and incorporated into the plans.

The process of contingency planning starts with the risk analysis of all information systems. The risk analysis should include all potential threats that could happen to an information system. Those include, but are not limited to, human (both intentional and unintentional) and non-human (natural disasters, animals, electrical or mechanical failures).

Once the risk analysis as been completed, a value should be placed on the assets. This gives management a clear understanding of what the SE stands to lose in the event of a potential loss of the system. This economic feasibility provides an understanding of the potential costs of the loss of the system, thereby giving guidance to a reasonable amount of redundancy, recovery services, or additional components/staff.

After a value is placed on the information system, a business impact analysis (BIA) should be completed to determine the impact of the outage on the business. The BIA takes into consideration both qualitative and/or quantitative analysis. The impact of an outage can be economic, either by fines or loss of revenue, or operational by not meeting the legal or perceived SE mission, or both. The BIA will help to prioritize those systems and functions and the order in which they will require attention in the event of a given incident.

Contingency planning should be focused on the SE's functions. When necessary, it is extremely important to document and manage interdependencies, not only within functions, but also between information systems and their components.

Requirements

CP-1 The SE develops, disseminates, and periodically reviews/updates:

1. A formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

CP-2 The SE develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.

CP-3 The SE trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*organization-defined frequency, at least annually*].

CP-4 The SE:

1. Tests and/or exercises the contingency plan for the information system [*organization-defined frequency, at*

	least annually] using [*organization-defined tests and/or exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan; and **2.** reviews the contingency plan test/exercise results and initiates corrective actions.
CP-5	The SE reviews the contingency plan for the information system [*organization-defined frequency, at least annually*] and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.
CP-6	The SE identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.
CP-7	The SE identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within [*organization-defined time period*] when the primary processing capabilities are unavailable.
CP-8	The SE identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within [*organization-defined time period*] when the primary telecommunications capabilities are unavailable.
CP-9	The SE conducts backups of user-level and system-level information (including system state information) contained in the information system [*organization-defined frequency*] and protects backup information at the storage location.
CP-10	The SE employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.

XXIII. Media Protection

The SE must:

1. Protect information system media, both paper and digital;
2. limit access to information on information system media to authorized users; and
3. sanitize or destroy information system media before disposal or release for reuse.

Media protection refers to those practices, technologies and/or services used to protect information and limit its disclosure. This includes, but is not limited to ensuring that; critical and/or sensitive information only resides on trusted servers which have adequate protections; information that travels outside of the SE's control is protected from disclosure by means of encryption; information is adequately destroyed, and information is adequately controlled by the SE.

Requirements

MP-1 The SE develops, disseminates, and periodically reviews/updates:

1. A formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

MP-2 The SE restricts access to information system media to authorized individuals.

MP-3 The SE:

1. Affixes external labels to removable information system media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information; and
2. exempts [organization-defined list of media types or hardware components] from labeling so long as they remain within [organization-defined protected environment].

MP-4 The SE physically controls and securely stores information system media within controlled areas.

MP-5 The SE protects and controls information system media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel.

MP-6 The SE sanitizes information system media, both digital and non- digital, prior to disposal or release for reuse.